# Perfect Security

Cryptography and Protocols
Andrei Bulatov

# Symmetric Encryption Scheme 对称加密方案

- A symmetric encryption scheme is a triple of algorithms (K,E,D)
  - K key generation
  - E encryption algorithm
  - D decryption algorithm
- For simplicity assume that k ← K uniformly at random, $k \in \{0,1\}^l$ or $k \in U_l$ bit string of length $l$.
- $P \in \{0,1\}^m$ plaintext

$$E:\{0,1\}^l \times \{0,1\}^m \rightarrow \{0,1\}^* \quad | \quad E_k(P) = C$$ 不同算法，长度不同 ciphertext

$$D:\{0,1\}^l \times \{0,1\}^* \rightarrow \{0,1\}^m \quad | \quad D_k(C) = P$$ plaintext

$$\{0,1\}^l \times (\{0,1\}^l \times \{0,1\}^*) = \{0,1\}^*$$

- In general, E is randomized, D is deterministic

Encryption algorithm is random

also called "Information theoritical security"

# Perfect Security

· 只是 keep key secure 是不行的.
例: ignore key, send the plaintext as cyphertext, it's not secure
· 只是让 attacker cannot recover the plaintext 也不行
例: Send all bits of the original plaintext except the last one, keep the last bit very secure, it's not secure.

- Let (K,E,D) be a symmetric encryption scheme. It is said to be perfectly secure if for any two plaintexts $P_1, P_2$ and a ciphertext C

$P_1$ & $P_2$ 有相同的概率被加密为C

$$\Pr[E_k(P_1) = C] = \Pr[E_k(P_2) = C],$$

where the probability is over the random choice $k \leftarrow K$, and also over the coins flipped by E

even attackers know 1 of 2 possible plaintext, and the cyphertext, there's no way to prefer one of the plaintext to the other.

## Security as a Game

全能的

- We assume that Eve is almighty
- Game
  - Alice chooses a key k
  - Eve chooses 2 plaintexts and gives them to Alice
    the 2 plaintext are easier for her
  - Alice encrypts one of them and sends to Eve
  - Eve decides which one is encrypted

  Eve wins if her decision is right $P_r = \frac{1}{2}$
- The system is perfectly secure if Eve wins with probability 1/2
- This notion of security is very strong:
  If Eve can do anything reasonable about CT, the system is insecure.

  Suppose that Eve can learn something about P. More precisely she can compute a function g(C) = f(P) $\in$ {0,1} ← only 1 bit

  Then she chooses $P_1, P_2$ with $f(P_1) \neq f(P_2)$

  → That's why the def don't allow Eve know sth about P.

# Example

- Let (K,E,D) be a substitution cipher over the alphabet $\Sigma$ consisting of 26 Latin letters. K picks a random permutation of $\Sigma$, that is $\pi \leftarrow \text{Perm}(\Sigma)$.

  The set of possible plaintexts is the set of all 3-letters English words.
- This SES is not perfectly secure.
- There are $P_1, P_2$ such that for some C

$$\Pr[E_k(P_1) = C] \neq \Pr[E_k(P_2) = C],$$

- Take $P_1$ = `FEE' and $P_2$ = `FAR', and C = `XYY'. Then

$$\Pr[E_k(P_1) = C] = \left[\text{prob. that } \mathrm{F} \to \mathrm{X}, \mathrm{E} \to \mathrm{Y}\right] = \frac{24!}{26!} = \frac{1}{25 \cdot 26}$$

$$\Pr[E_k(P_2) = C] = 0$$

same as horse race example

F→X, E→Y, 其它字母排列的方法有 24! 种

## One-Time Pad

- The one-time pad is the following cryptosystem $(K, E, D)$:
  - $k \leftarrow K$ uniformly at random from $\{0,1\}^m$
  - the set of possible plaintexts is $\{0,1\}^m$
  - $E: \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}^m$

    $P = P^1 \dots P^m$, $\quad k = k^1 \dots k^m$

    $C = C^1 \dots C^m$, $\quad$ where $C^i = P^i \oplus k^i (mod\ 2)$
  - $D: \{0,1\}^m \times \{0,1\}^m \rightarrow \{0,1\}^m$

    $P^i = C^i \oplus k^i (mod\ 2)$

$k \oplus c = k \oplus (k \oplus m) = (k \oplus k) \oplus m = 0 \oplus m = m$

# Perfect Security of OTP

- **Theorem.**

  The OTP is perfectly secure

- **Proof.**

  For any $P_1, P_2, C \in \{0,1\}^m$ we have to prove that

$$\Pr[E_k(P_1) = C] = \Pr[E_k(P_2) = C],$$

Indeed,

$$\Pr[E_k(P_1) = C] = \Pr[k \oplus P_1 = C]$$

only 1 key possible

$$= \frac{|\{k \in \{0,1\}^m : k \oplus P_1 = C\}|}{|\{0,1\}^m|} = \frac{1}{2^m}$$

$$\Pr[E_k(P_2) = C] = \frac{1}{2^m}$$

缺: $|k| \geq |P|$

If the key can be sent securely, the P can be send securly.

# Short Key – No Security

- **Theorem**

  There is no perfectly secure SES with m-bit messages and m – 1 –bit keys

- **Proof (optional)**

  Suppose (K,E,D) is such SES.

  all possible keys

  Set $S_0 = \{E_k(0^m) | k \in \{0,1\}^{m-1}\}$

  小于：可能有2个key加密成相同的c

  Since $\left|\{0,1\}^{m-1}\right| = 2^{m-1}$, we have $|S_0| \leq 2^{m-1}$ 1 key → 1 ciphertext

  Choose $C \notin S_0$ and $P$ such that there is key $k$ with $E_k(P) = C$

  ↳ since all plaintext with m bits should have different ciphertext with the same key (otherwise, cannot decrypt), then there're $2^m$ ciphertext

  Then

  $$\Pr[E_k(0^m) = C] = 0, \quad \text{while}$$

  $$\Pr[E_k(P) = C] > 0$$